New and improved

Tore Frederiksen, Thomas Jakobsen, Jesper Nielsen and Roberto Trifiletti

AARHUS UNIVERSITY
The problem:

- Do you love secure computation?
- Do you need security strong enough to withstand malicious attacks?
- Do you need flexibility enough to be able to evaluate any efficiently computable Boolean circuit?
- Do you want constant round complexity?
- Do you want asymptotic efficiency?

* Lego is a product of Jesper Nielsen and Claudio Orlandi introduced at TCC 2009
That can be solved!

• Do you want OT-hybrid security using only asymmetric calls linear in the security parameter?

* MiniLego is a product of Tore Frederiksen, Thomas Jakobsen, Jesper Nielsen, Peter Nordholt and Claudio Orlandi introduced at Eurocrypt 2013
Can this be improved??

- Introducing the all **new** and **improved** Lego protocol..

Kind of like MiniLEGO... only with small constants and support for preprocessing
How?! – MiniLEGO recap

- Construct many garbled gates and solder them together to form fault tolerant buckets (majority rules)
- Solder the buckets together
- Evaluate like any garbled circuit
- *But* to solder MiniLEGO needs XOR homomorphic commitments on each 0-key of each wire in each gate along with a global difference
- These are done using OT extension and error correcting codes and result in large constants
Our magic!

• We have removed the need for “strong” XOR-homomorphic commitments
• We add commitments (hashes) to each key
• We evaluate using “key sets”
Our magic!

- Commitments don’t need error correcting codes and are much, much smaller
- Only need one “good” gate per bucket, not majority

* Using the idea of forge-and-loose introduced in [B13, HKE13, L13]
Recap

• We offer malicious security, constant round complexity, limited use of asymmetric primitives and asymptotic and practical efficiency*

• 100% free from semi/fully homomorphic primitives, obfuscation and specific number theoretic assumptions

*Subject to implementation
• Still a work in progress, but expect it on ePrint before Christmas

*Subject to the probability distribution induced by peer review*